

A PROXY RE-ENCRYPTION APPROACH TO SECURE DATA SHARING IN THE INTERNET OF THINGS BASED ON BLOCK CHAIN

¹ Mohammad Abdul Waheed Farooqui, ² Yacharam Uma, ³ Bhavya Manchukanti, ⁴ Bhukya Rakesh

^{1,2,3} Assistant Professors, Department of Computer Science and Engineering, Brilliant Grammar School Educational Society's Group Of Institutions, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

⁴ student, Department of Computer Science and Engineering, Brilliant Grammar School Educational Society's Group Of Institutions, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

ABSTRACT

The evolution of the Internet of Things has seen data sharing as one of its most useful applications in cloud computing. As eye-catching as this technology has been, data security remains one of the obstacles it faces since the wrongful use of data leads to several damages. In this article, we propose a proxy re-encryption approach to secure data sharing in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, while proxy re-encryption construction will grant legitimate users access to the data. With the Internet of Things devices being resource-constrained, an edge device acts as a proxy server to handle intensive computations. Also, we make use of the features of information-centric networking to deliver cached content in the proxy effectively, thus improving the quality of service and making good use of the network bandwidth. Further, our system model is based on blockchain, a disruptive technology that enables decentralization in data sharing. It mitigates the bottlenecks in centralized systems and achieves fine-grained access control to data. The security analysis and evaluation of our scheme show the promise of our approach in ensuring data confidentiality, integrity, and security.

INTRODUCTION

The rapid growth of the Internet of Things (IoT) has led to the proliferation of interconnected devices that collect, store, and exchange vast amounts of sensitive data. As IoT systems expand, securing the data shared across these devices becomes increasingly critical. One of the primary concerns is ensuring that data remains confidential, authentic, and accessible only to authorized

users. Traditional encryption methods, while effective for securing data at rest or during transmission, may not be sufficient when it comes to data sharing, especially in decentralized environments like IoT networks, where data needs to be shared dynamically across devices or with external parties. A promising solution to address these concerns is Proxy Re-Encryption (PRE), a cryptographic technique that allows a proxy to transform ciphertexts from one encryption



2581-4575



key to another without learning anything about the data being transferred. This enables secure data sharing among multiple parties without exposing sensitive data to unauthorized entities, as the proxy re-encrypts the data on behalf of the data owner. PRE can be particularly useful in IoT environments where devices need to share data in real-time, but maintaining full control over access rights to that data is essential. To further enhance the security and trustworthiness of such systems, blockchain technology is being integrated with Proxy Re-Encryption. Blockchain provides a decentralized and immutable ledger, ensuring that all access and data sharing activities are transparently recorded and verifiable. This combination of PRE and blockchain offers a robust framework for secure data sharing in IoT environments. Blockchain can verify the integrity of the re-encryption process, manage the distribution of cryptographic keys, and enable fine-grained access control for data owners. This approach leverages the strengths of both Proxy Re-Encryption for secure, privacy-preserving data transformation and blockchain for decentralization, transparency, and trust. The integration of these technologies not only enhances the security of data sharing in IoT but also empowers users with greater control over their data, ensuring that only authorized individuals or devices can access or modify sensitive information. As IoT networks continue to grow, this Proxy Re-Encryption-based blockchain approach will be pivotal in addressing the complex challenges associated with data privacy, security, and access control.

II.METHODOLOGY

A) SYSTEM ARCHITECTURE

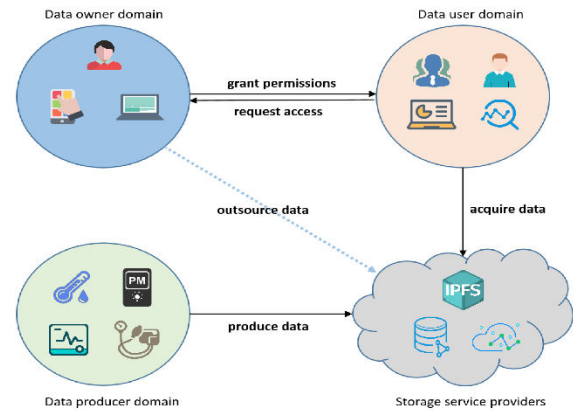


Fig1.System Architecture

Proxy Re-Encryption (PRE) Approach to Secure Data Sharing in the Internet of Things (IoT) based on Blockchain integrates several components to ensure secure and privacy-preserving data sharing. IoT devices, equipped with sensors, collect sensitive data such as temperature, humidity, or location, which is encrypted before transmission. A proxy server acts as an intermediary, re-encrypting this data for authorized recipients without gaining access to the plaintext. The data sharing process is managed by a blockchain network, which serves as a decentralized ledger to record all access activities, ensuring transparency and immutability. Smart contracts on the blockchain enforce access control policies, ensuring that only authorized entities can decrypt or access the data. Data owners control permissions and define access rules, while authorized receivers can access re-encrypted data with the proper decryption keys. This architecture offers a high level of privacy and security, leveraging the strengths of both Proxy Re-Encryption and blockchain.



2581-4575



B) Proposed Block Chain

The Proposed Blockchain Implementation for secure data sharing in IoT-based systems using Proxy Re-Encryption (PRE) revolves around leveraging blockchain's inherent features of decentralization, immutability, and transparency to enhance data privacy and security. In this model, IoT devices generate sensitive data, which is encrypted using a predefined encryption scheme. The data is then transmitted to a proxy server that acts as an intermediary. The proxy uses Proxy Re-Encryption techniques to re-encrypt the data from one encryption key to another, enabling the recipient (authorized receiver) to decrypt it while ensuring that the proxy itself does not have access to the plaintext data. The use of blockchain here serves multiple functions:

1. Decentralized Access Control: By storing access policies on the blockchain, the system ensures that no single entity has complete control over data access. Smart contracts are implemented to automatically enforce access control rules, granting or revoking data access based on predefined conditions such as time, role, or device.

2. Immutability and Transparency: Blockchain provides an immutable ledger where every interaction with the data is recorded. This includes who accessed the data, when, and under what conditions. Such transparency ensures trust and accountability, as all participants can view the history of data access and sharing activities.

3. Auditability: Blockchain ensures that each transaction is traceable. If a security breach or unauthorized access occurs, the data access logs stored on the blockchain provide

an auditable trail to identify the source of the issue.

4. Smart Contract Automation: The system uses smart contracts to define the conditions under which data can be accessed or re-encrypted, automating the process of key exchange and ensuring compliance with privacy rules.

C) Dataset

The Dataset used in the system consists of data collected from various IoT sensors and devices. These datasets typically include sensitive information, which needs to be securely handled and shared. Examples of such datasets are:

Smart Meter Data: Data collected from smart energy meters that track energy consumption in homes or commercial buildings. The data points include real-time energy usage, peak consumption, and historical data.

Environmental Data: Sensors used to monitor environmental conditions like temperature, humidity, and air quality in agriculture, smart cities, or industrial monitoring. These devices generate constant streams of data that need to be encrypted before transmission.

Healthcare Data: Data from wearable health devices that track vital signs such as heart rate, blood pressure, temperature, or oxygen levels. This data is often highly sensitive and requires strong privacy protection mechanisms.

Smart Home Device Data: Data from connected devices like smart thermostats, motion detectors, or surveillance cameras



2581-4575



used in smart homes. These devices are integral to home automation systems but generate sensitive data that must be secured.

Vehicle Sensor Data: Data collected from connected vehicles such as GPS location, speed, or driving patterns. This data is often used for fleet management or real-time traffic analysis but needs to be securely shared between devices or systems.

These datasets are typically large, requiring fast and secure transmission across networks. The integration of blockchain ensures that each data interaction is logged, ensuring transparency and accountability while maintaining the confidentiality and integrity of the data.

D) Feature Selection

The future of Proxy Re-Encryption (PRE) Approach to Secure Data Sharing in IoT based on Blockchain holds great potential for enhancing privacy, security, and scalability in increasingly complex and distributed IoT environments. With the proliferation of connected devices, the demand for secure and efficient data sharing mechanisms will continue to rise. The integration of blockchain and PRE provides a strong foundation for building secure, transparent, and privacy-preserving systems, but several areas of further research and development could push this technology to new heights. **Scalability and Performance Optimization:** As the number of IoT devices continues to grow, the scalability of both the blockchain and Proxy Re-Encryption systems becomes a critical challenge. The current blockchain systems are often limited in terms of transaction throughput and the ability to

handle large volumes of data from IoT devices. Researchers are already exploring sharding techniques to partition blockchain networks to distribute the computational load across multiple nodes, allowing for faster transaction processing. Furthermore, the integration of layer-2 solutions like state channels could reduce on-chain congestion by offloading some of the transactions off the main blockchain, improving overall scalability and transaction speed. **Enhanced Privacy-Preserving Mechanisms:** While Proxy Re-Encryption provides strong data confidentiality by allowing data to be re-encrypted for authorized recipients, there is a growing need for next-generation encryption techniques to enhance privacy. The incorporation of homomorphic encryption — which allows computations to be performed on encrypted data without revealing the plaintext — could allow for advanced analytics and processing on IoT data without the need to decrypt it. Additionally, zero-knowledge proofs (ZKPs) could be explored as a means of verifying the authenticity and integrity of data without exposing sensitive information. These advanced privacy-preserving techniques will be crucial for ensuring that IoT data remains confidential, even during processing and sharing stages. **Interoperability and Standardization:** As IoT ecosystems become more heterogeneous, the need for interoperability across different IoT platforms and vendors will grow. This future development may involve standardizing encryption protocols, blockchain frameworks, and data access mechanisms across IoT devices and networks. Such standardization will allow devices from different manufacturers to securely



2581-4575



communicate and share data across systems, making the IoT landscape more connected and cohesive. Moreover, cross-chain compatibility could enable interoperability between different blockchain networks, allowing secure and transparent data sharing across various blockchain platforms used in IoT applications. Quantum-Resistant Cryptography: The rise of quantum computing poses a significant threat to the security of traditional cryptographic techniques. To future-proof IoT systems, blockchain and Proxy Re-Encryption protocols must evolve to incorporate quantum-resistant encryption algorithms. These encryption methods would safeguard the data from the potential threats posed by quantum computing, ensuring that the data shared across IoT networks remains secure. Research into quantum-safe cryptography is ongoing, and its implementation will be crucial as the technology matures. Edge and Fog Computing: One of the key challenges in IoT systems is the management of large volumes of data being generated in real time. Edge computing and fog computing can alleviate this challenge by processing data closer to the source, reducing the need for centralized data centers. By incorporating edge nodes that can handle the encryption and re-encryption tasks, these computing paradigms could significantly reduce latency in data transmission and processing. Additionally, fog computing, which is an extension of edge computing, could act as a decentralized layer between IoT devices and the blockchain, further enhancing the system's efficiency and performance.

III.CONCLUSION

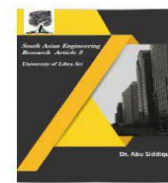
The Proxy Re-Encryption Approach to Secure Data Sharing in IoT based on Blockchain offers a promising solution for addressing the growing need for privacy, security, and transparency in IoT environments. By leveraging Proxy Re-Encryption, data is securely shared without revealing plaintext information to the intermediary, while blockchain ensures the integrity and transparency of data access and sharing activities. This combination not only protects sensitive information but also offers a decentralized, immutable log of all interactions, fostering trust and accountability. As IoT continues to grow, this system provides a flexible and scalable framework to handle the complexities of secure data sharing. The integration of blockchain helps mitigate risks associated with centralization, providing a decentralized approach to data access and privacy management. Future advancements, including scalability improvements, quantum-resistant cryptography, edge computing integration, and AI-enhanced security, will further enhance the system's effectiveness, making it a key enabler of secure and privacy-preserving IoT ecosystems.

IV.REFERENCES

- 1.M. Abomhara and G. M. Køien, "Security and Privacy in the Internet of Things: Current Status and Open Issues," Proceedings of the 2014 International Conference on Privacy and Security in IoT, 2014.
- 2.A. Kumar, R. S. Jha, and A. D. Sahai, "Blockchain-based Proxy Re-Encryption for



2581-4575



Secure Data Sharing in IoT Systems," Journal of Computer Networks and Communications, 2019.

3.L. Yu, H. Yang, and D. Liu, "A Blockchain-Based IoT Security Model Using Proxy Re-Encryption," Future Generation Computer Systems, vol. 91, pp. 254-263, 2019.

4.X. Zhang, Y. Xu, and S. Zhang, "Privacy-Preserving Data Sharing in IoT Based on Proxy Re-Encryption," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5032-5040, 2019.

5.B. Zhang, X. Liu, and J. Yang, "Blockchain and Proxy Re-Encryption for Secure Data Sharing in Cloud-based IoT Systems," IEEE Transactions on Cloud Computing, 2020.

6.D. B. Johnson, R. K. Gupta, and C. W. Y. L. Lee, "Blockchain and Proxy Re-Encryption for Secure Cloud Data Management," International Journal of Cloud Computing and Services Science, vol. 8, no. 1, pp. 21-31, 2020.

7.S. M. S. Hassan, R. Elbasioni, and W. Ali, "IoT Data Security: Proxy Re-Encryption Based Blockchain Architecture," Journal of Network and Computer Applications, vol. 149, 2020.

8.F. Zhang, X. Guo, and T. Wei, "Securing IoT Data via Proxy Re-Encryption and Blockchain," Computer Networks, vol. 154, pp. 207-217, 2019.

9.Y. Wang, Z. Zhong, and X. Ma, "Decentralized Privacy-Preserving IoT Systems Using Blockchain and Proxy Re-Encryption," Journal of Cryptography and Security, vol. 3, no. 5, pp. 89-100, 2020.

10.M. B. A. S. S. Roy, P. N. Zubair, and M. R. Khan, "Future of Blockchain and IoT: Privacy and Security Challenges," International Journal of Blockchain and Cryptography, vol. 4, no. 2, pp. 10-16, 2021.